A Response to the Question About the Need for CREN Products and Services

Posed by Michael Gettes at the Common Solutions Group Meeting, 15-17 January 2003, Austin, Texas

At the Common Solutions Group meeting Michael Gettes asked why CREN's support of digital certificates should be continued if there were commercial solutions available. After some time to consider Michael's question, I wanted to respond in the thoughtful way he had posed it.[1] Those who read this reply should be aware that we had discussed the Immigration and Naturalization Services' requirement that colleges and universities with foreign students must have at least one VeriSign Class 1 digital certificate to conduct business with the agency.[2] In an early 2002 letter to the INS, CREN had suggested that colleges and universities be permitted to use CREN digital certificates. The INS did not respond. The INS also did not use federal ACES certificates for their SEVIS (Student and Exchange Visitor Information System) implementation.

First, integration with the campus admissions and registration process. The most expensive part of issuing digital certificates appears to be the identification process itself. In higher education this cost is already borne by the admissions or registration process. (This does not imply there is a single registration process or a single level of assurance). For example, CREN was considering issue certificates to faculty, staff, and students based on a request from a campus—relying on the campus' identification of the person. This is especially important for a small campus that needs personal digital certificates, but does not have its own certificate authority.

Second, controlled naming. It is important for a college or university to know no one else will be issued a digital certificate with a similar institutional name. (This is at least one incident where a commercial firm registered a digital certificate to a person with a corporate name similar to a major firm). It would be helpful if institutional names were checked against the federal directories of colleges and universities to avoid unintended ambiguity. (such as the National Student Clearinghouse's use of the U.S. Department of Education's PEPS database).

Third, considerable research and development was needed to establish policies and practices for the use of digital certificates. At CREN this was done in the specific context of higher education, I believe this work is important for those colleges and universities considering to adopt, or forced to adopt, digital certificates. The experience of the Massachusetts Institute of Technology and the current project at Dartmouth College

---

[1] The JA-SIG Board does not now have a position on CREN products or services. This is a personal perspective.

[2] "VeriSign Class 1 Individual Certificates modestly enhances the security of some of these applications by assuring that a certificate's subject and e-mail address are included unambiguously within VeriSign's repository. Class 1 Certificates provide assurances that communications originate from a particular source. Class 1 Certificates **do not provide proof of identity**." From VeriSign's PKI Disclosure Statement, Version 1 copied from http://www.verisign.com/repository/disclosure.html, January 30, 2003. Emphasis in the original document.

suggest practices in higher education that differ from commercial practice. The CREN efforts build upon these experiences in higher education.

Fourth, the University of California has been advocating the need for digital certificates that are linked to their authorization system, but do not reveal identity. This may require coordination and cooperation with the issuing authority, but has not been important to commercial firms. This is part of the University of California concern that readers of digital materials be authorized access, but not personally identified. Anonymous use sustains a library policy, but is not important in the commercial world.

Fifth, moving from no use of digital certificates to becoming a certificate authority or from server use to personal use may need to be done in steps. The CREN products as outlined in the CREN Business Plan support this migration and transition.

Sixth, reasonable price. The current pricing of commercial services, such as VeriSign, becomes very expensive with a number of servers—now averaging 22 per campus—and with the potential use by the entire student body.

Seventh, maintenance of a directory of colleges and universities and their associated public keys, preferably as an extension of a UDDI server supporting Web services, is important to facilitate data exchange. And potential links between this directory and directories on campus using MACE technology, would facilitate the use of personal digital certificates for document authentication.

Eighth, special profiles. Higher education may need certificates with profiles or periods of validity that differ from commercial practice, such as the 13 month or 15 month periods suggested for journal access.

Higher education is both a small and specialized market. From the ERP software vendors we have learned when higher education requirements differ from their commercial customers, the ERP vendors tend to respond to the commercial requirements. Because of the high marketing expenses of the commercial security firms, a focused higher education effort may be more efficient.